ASA 8.X:AnyConnect登入前啟動功能配置

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[慣例](#)
[背景資訊](#)
[登入前安裝啟動元件（僅限Windows）](#)
[Windows-Vista\Windows 7和Pre-Vista Start Before Logon之間的區別](#)
[啟用SBL的XML設定](#)
[啟用SBL](#)
[使用CLI啟動登入前配置](#)
[使用ASDM在登入前啟動配置](#)
[使用清單檔案](#)
[排除SBL故障](#)
[問題1](#)
[解決方案1](#)
[相關資訊](#)

簡介

啟用*Start Before Logon*(SBL)後，使用者會在Windows®登入對話方塊出現之前看到AnyConnect GUI登入對話方塊。首先建立VPN連線。Start Before Logon僅適用於Windows平台，管理員可以控制登入指令碼的使用、密碼快取、將網路驅動器對映到本地驅動器等。您可以使用SBL功能啟用VPN，作為登入序列的一部分。預設情況下，SBL處於禁用狀態。

有關配置AnyConnect VPN客戶端功能的詳細資訊，請參閱配置AnyConnect客戶端功能部分。

注意：在AnyConnect客戶端中，您對SBL執行的唯一配置是啟用該功能。網路管理員根據其情況的要求處理登入前進行的處理。可以將登入指令碼分配給域或單個使用者。通常，域管理員具有批處理檔案或類似檔案，這些檔案或類似檔案在Active Directory中是由使用者或組定義的。使用者登入後，即會執行登入指令碼。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行軟體版本8.x的Cisco ASA 5500系列自適應安全裝置
- Cisco AnyConnect VPN版本2.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

SBL的要點是，在登入到PC之前，它將遠端電腦連線到公司基礎設施。例如，使用者可能位於公司物理網路之外，在其個人電腦加入公司網路之前無法訪問公司資源。啟用SBL後，AnyConnect客戶端會在使用者看到Microsoft登入視窗之前進行連線。使用者還必須像往常一樣在Microsoft登入視窗出現時登入到Windows。

以下是使用SBL的幾個原因：

- 使用者的PC已加入Active Directory基礎設施。
- 使用者在PC上不能有快取的憑據，即如果組策略不允許快取的憑據。
- 使用者必須運行從網路資源執行或需要訪問網路資源的登入指令碼。
- 使用者具有網路對映驅動器，需要使用Active Directory基礎架構進行身份驗證。
- 網路元件（如MS NAP/CS NAC）可能需要連線到基礎設施。

SBL建立的網路相當於包含在本地企業LAN中。啟用SBL後，由於使用者可以訪問本地基礎架構，因此遠端使用者也可以使用通常在辦公室中為使用者運行的登入指令碼。

有關如何建立登入指令碼的資訊，請參閱此Microsoft TechNet文章 。

有關如何在Windows XP中使用本地登入指令碼的資訊，請參閱此Microsoft文章 。

在另一個示例中，可以將系統配置為禁止快取的憑證以登入到PC。在這種情況下，使用者必須能夠與企業網路上的域控制器通訊，以便在訪問PC之前驗證其憑據。SBL要求在呼叫時存在網路連線。在某些情況下，這是不可能的，因為無線連線可能依賴於使用者憑證來連線到無線基礎架構。由於SBL模式在登入的憑據階段之前，因此在此場景中連線不可用。在這種情況下，需要配置無線連線以跨登入快取憑證，或者需要配置其他無線身份驗證以使SBL正常工作。

登入前安裝啟動元件（僅限Windows）

必須在安裝核心客戶端之後安裝「登入前啟動」元件。此外，AnyConnect 2.2 Start Before Logon元件要求安裝2.2版或更高版本的核心AnyConnect客戶端軟體。如果使用MSI檔案預部署AnyConnect客戶端和「登入前啟動」元件(例如，您所在的大公司擁有自己的軟體部署（Altiris、Active Directory或SMS），則必須正確獲取訂單。如果管理員載入了AnyConnect（如果已進行Web部署和/或Web更新），系統會自動處理安裝順序。有關完整安裝資訊，請參閱Cisco AnyConnect VPN客戶端版本2.2的發行說明。

Windows-Vista\Windows 7和Pre-Vista Start Before Logon之間的區別

在Windows Vista和Windows 7系統上啟用SBL的步驟略有不同。Pre-Vista系統使用稱為虛擬專用網路圖形識別和身份驗證(VPNGINA)的元件來實施SBL。Vista和Windows 7系統使用名為PLAP的元件來實施SBL。

在AnyConnect客戶端中，Windows Vista登入前啟動功能稱為登入前訪問提供程式(PLAP)，它是可連線的憑據提供程式。此功能允許網路管理員在登入前執行特定任務，如收集憑證或連線到網路資源。PLAP在Windows Vista、Windows 7和Windows 2008 Server上提供「登入前啟動」功能。PLAP分別支援vpnplap.dll和vpnplap64.dll作業系統的32位和64位版本。PLAP功能支援Windows Vista x86和x64版本。

注意：在本節中，VPNGINA指的是Vista之前平台的「登入前啟動」功能，而PLAP指的是Windows Vista和Windows 7系統的「登入前啟動」功能。

在pre-Vista系統中，「登入前啟動」使用名為VPN圖形識別和身份驗證動態連結庫(vpngina.dll)的元件提供「登入前啟動」功能。Windows PLAP元件是Windows Vista的一部分，它取代了Windows GINA元件。

當使用者按Ctrl+Alt+Del組合鍵時，GINA會被啟用。使用PLAP時，Ctrl+Alt+Del組合鍵將開啟一個視窗，使用者可以在此視窗右下角使用「網路連線」按鈕選擇登入系統或啟用任何網路連線（PLAP元件）。

接下來的幾節將介紹VPNGINA和PLAP SBL的設定和過程。有關在Windows Vista平台上啟用和使用SBL功能(PLAP)的完整說明，請參閱在Windows Vista系統上配置登入前啟動(PLAP)。

啟用SBL的XML設定

UseStartBeforeLogon的元素值允許開啟(true)或關閉(false)此功能。 如果在配置檔案中將此值設定為**true**，則登入序列中還會進行其他處理。有關其他詳細資訊，請參閱登入前啟動說明。將CiscoAnyConnect.xml檔案中的<UseStartBefore Logon>值設定為**true**以啟用SBL:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
```

若要禁用SBL，請將相同的值設定為**false**。

若要啟用UserControllable功能，請在啟用SBL時使用以下語句：

```
<UseStartBeforeLogon userControllable="false">true</UseStartBeforeLogon>
```

與此屬性關聯的任何使用者設定都儲存在其他位置。

啟用SBL

為了最大限度地縮短下載時間，AnyConnect客戶端只請求下載（從安全裝置）其支援的每個功能所需的核心模組。要啟用新功能（例如SBL），您必須在組策略WebVPN或使用者名稱WebVPN配置模式下使用**svc modules**命令指定模組名稱：

```
[no] svc modules {none | value string}
```

SBL的字串值為**vpngina**。

在本示例中，網路管理員進入組策略遠端工作者的組策略屬性模式；進入組策略的WebVPN配置模式；並指定字串VPNGINA以啟用SBL:

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)# svc modules value vpngina
```

此外，管理員必須確保AnyConnect <profile.xml>檔案（其中<profile.xml>是網路管理員分配給XML檔案的名稱）將<UseStartBeforeLogon>語句設定為**true**，例如：

```
UseStartBeforeLogon UserControllable="false">true
```

必須在「登入前啟動」生效之前重新啟動系統。您還必須在安全裝置上指定允許SBL的模組，或任何其它模組，以獲得其他功能。如需詳細資訊，請參閱為其他AnyConnect功能啟用模組（第2-5頁，ASDM）部分或為其他AnyConnect功能啟用模組（第3-4頁，CLI）中的說明。

使用CLI啟動登入前配置

此案例說明如何使用CLI設定XML檔案：

1. 建立要下推到客戶端PC的配置檔案，該配置檔案如下所示：

```
<?xml version="1.0" encoding="UTF-8" ?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi :schemaLocation=
   "http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>text.cisco.com</HostName>
</HostEntry>
<HostEntry>
<HostName>test1.cisco.com</HostName>
<HostAddress>1.1.1.1</HostAddress>
</HostEntry>
.
.
.
<HostEntry>
<HostName>test2.cisco.com</HostName>
<HostAddress>1.1.1.2</HostAddress>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

2. 將檔案複製到安全裝置上的快閃記憶體中：

```
Copy tftp://x.x.x.x/AnyConnectProfile.xml AnyConnectProfile.xml
```

3. 在安全裝置上，將配置檔案作為可用配置檔案新增到WebVPN全區域性分，前提是所有其他內容均已正確設定用於AnyConnect連線：

```
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)#
   svc profiles ReallyNewProfile disk0:/AnyConnectProfile.xml
```

4. 編輯所使用的組策略，並新增**svc modules**和**svc profile**命令：

```
hostname(config)# group-policy GroupPolicy internal
hostname(config)# group-policy GroupPolicy attributes
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)# svc modules value vpngina
hostame(config-group-webvpn)# svc profiles value ReallyNewProfile
```

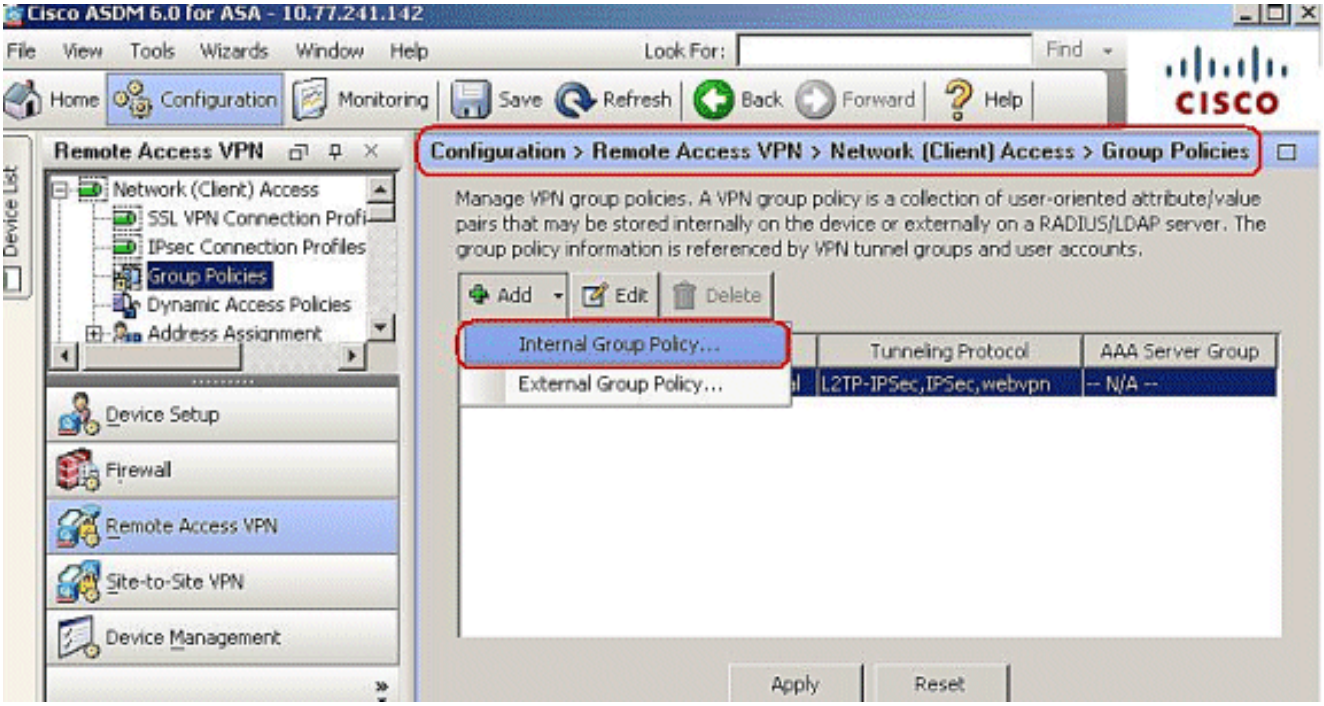
使用ASDM在登入前啟動配置

完成以下步驟，使用ASDM配置SBL:

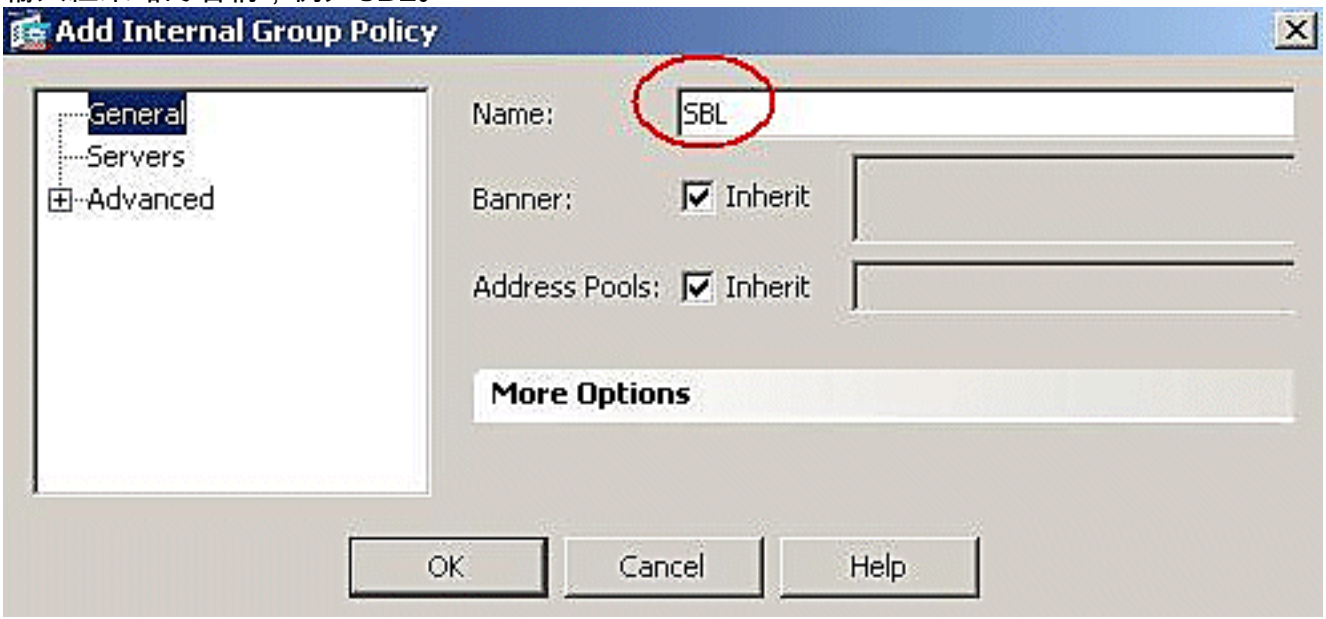
1. 建立要下推到客戶端PC的配置檔案，該配置檔案如下所示：

```
<?xml version="1.0" encoding="UTF-8" ?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi :schemaLocation=
   "http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>text.cisco.com</HostName>
</HostEntry>
<HostEntry>
<HostName>test1.cisco.com</HostName>
<HostAddress>1.1.1.1</HostAddress>
</HostEntry>
.
.
.
<HostEntry>
<HostName>test2.cisco.com</HostName>
<HostAddress>1.1.1.2</HostAddress>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

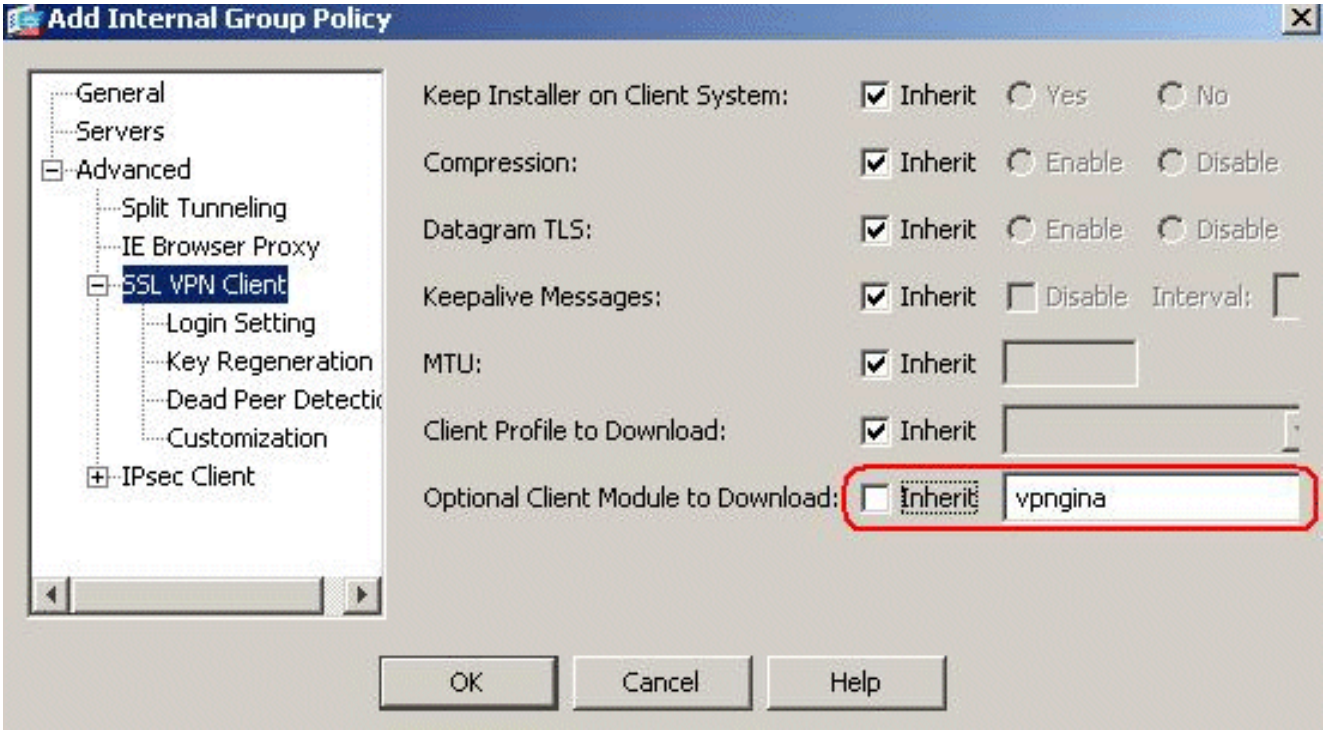
2. 在本地電腦中將配置檔案另存為**AnyConnectProfile.xml**。
3. 啟動ASDM，然後轉到首頁。
4. 轉到**Configuration > Remote Access VPN > Network(Client)Access > Group Policies > Add**，然後點選**Internal Group Policy**。



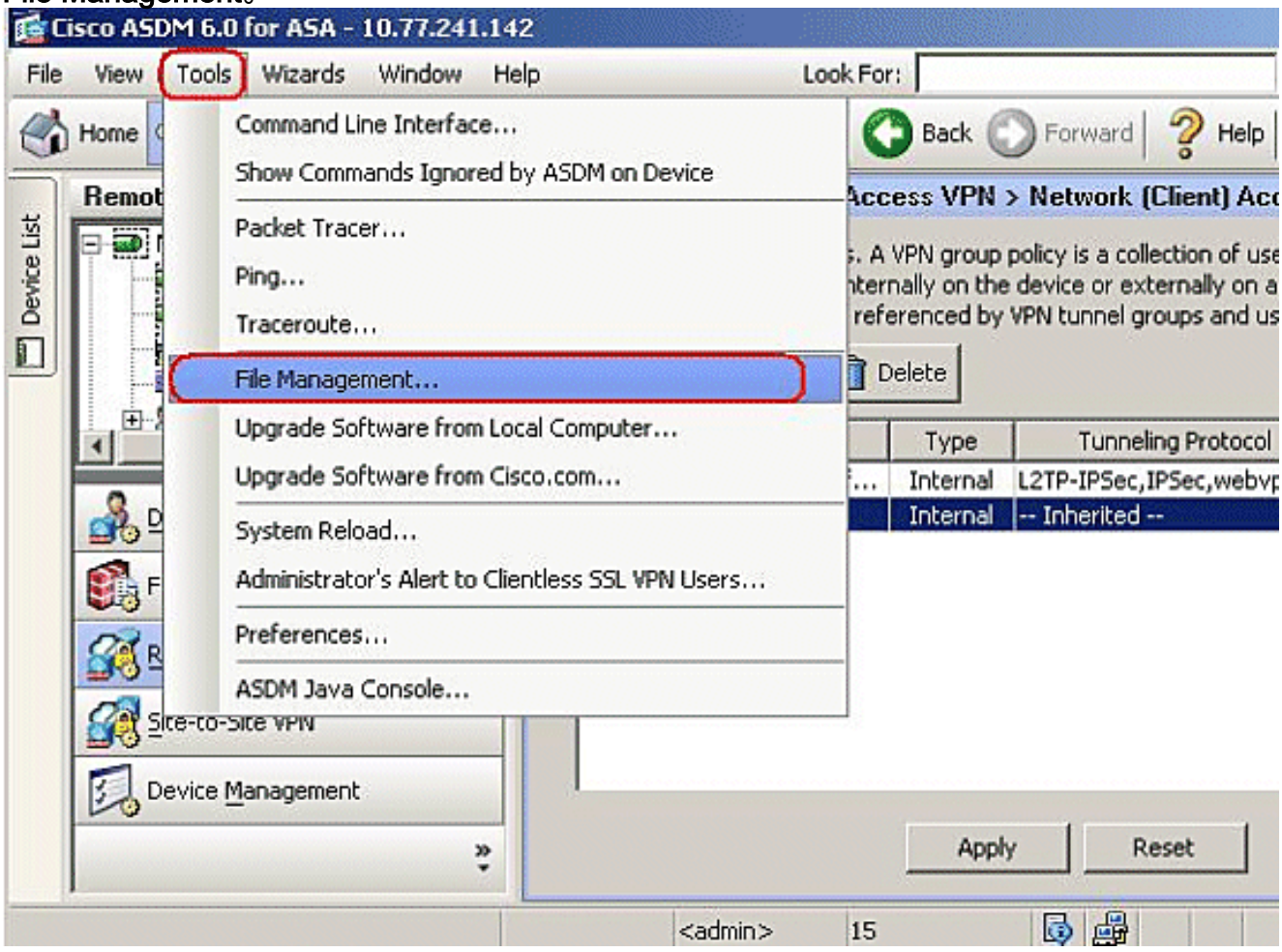
5. 輸入組策略的名稱，例如**SBL**。



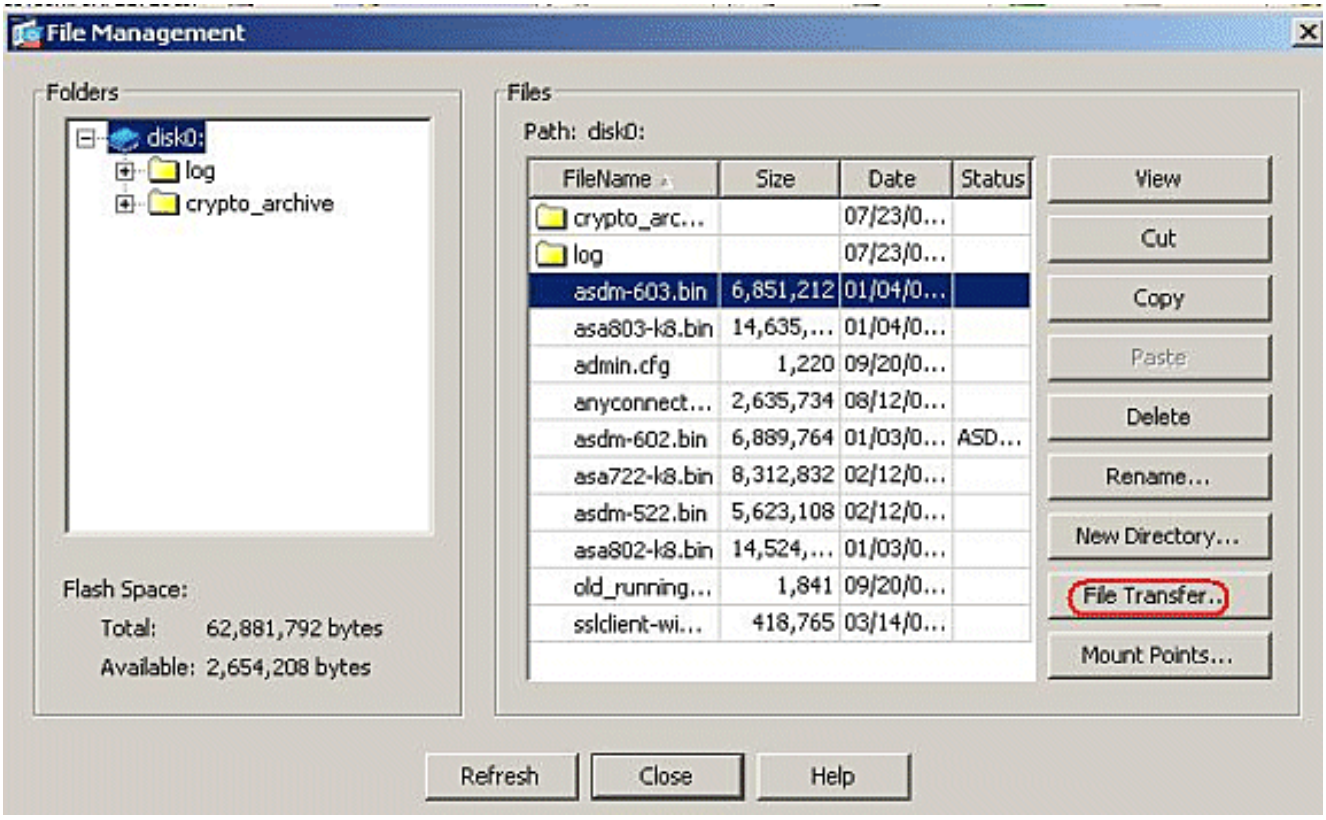
6. 轉至**Advanced > SSL VPN Client**。移除**Optional Client Module to Download**中的Inherit複選標籤，然後從下拉框中選擇**vpngina**。



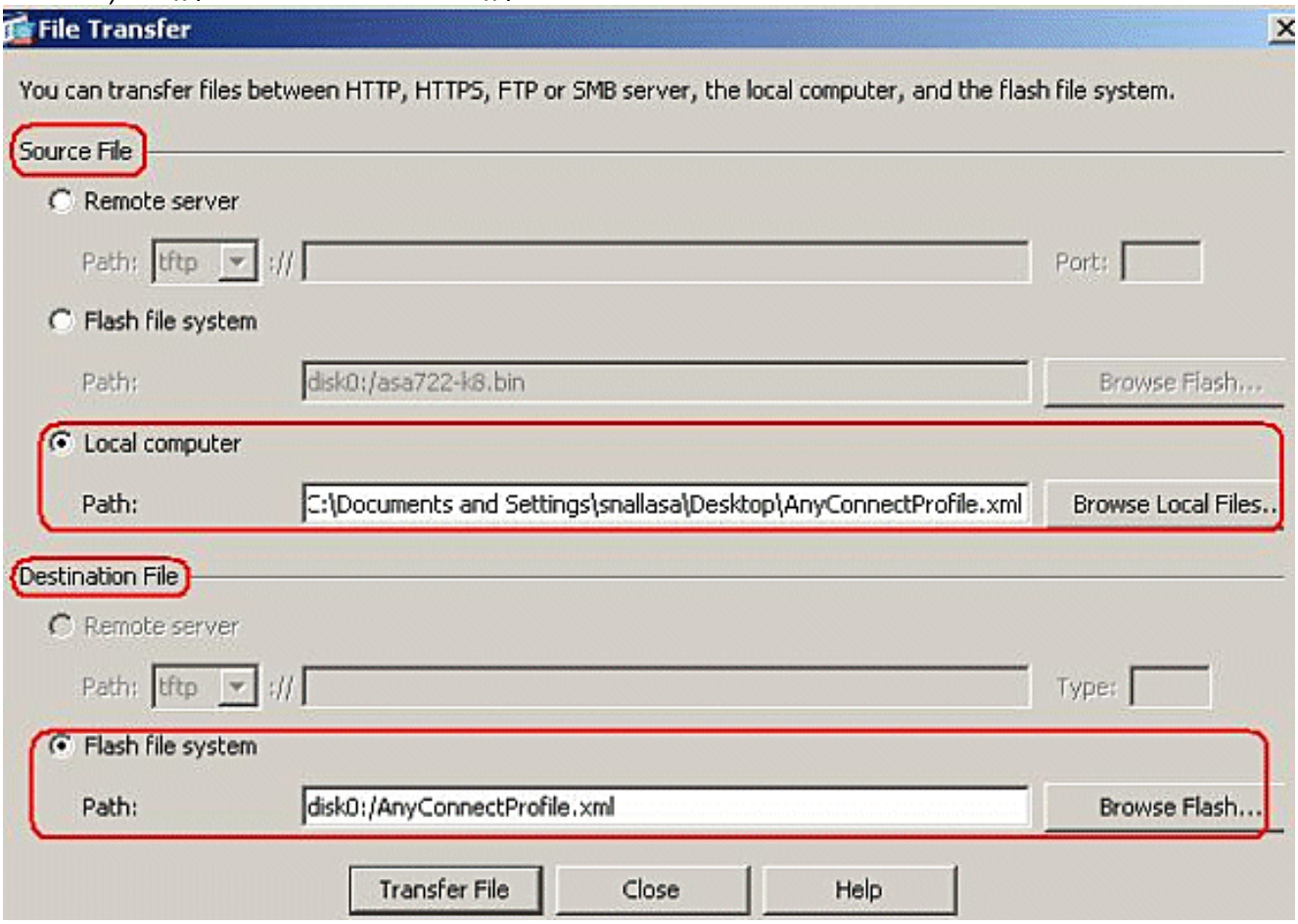
7. 若要將配置檔案**AnyConnectProfile.xml**從本地電腦傳輸到Flash，請轉到**Tools**，然後按一下**File Management**。



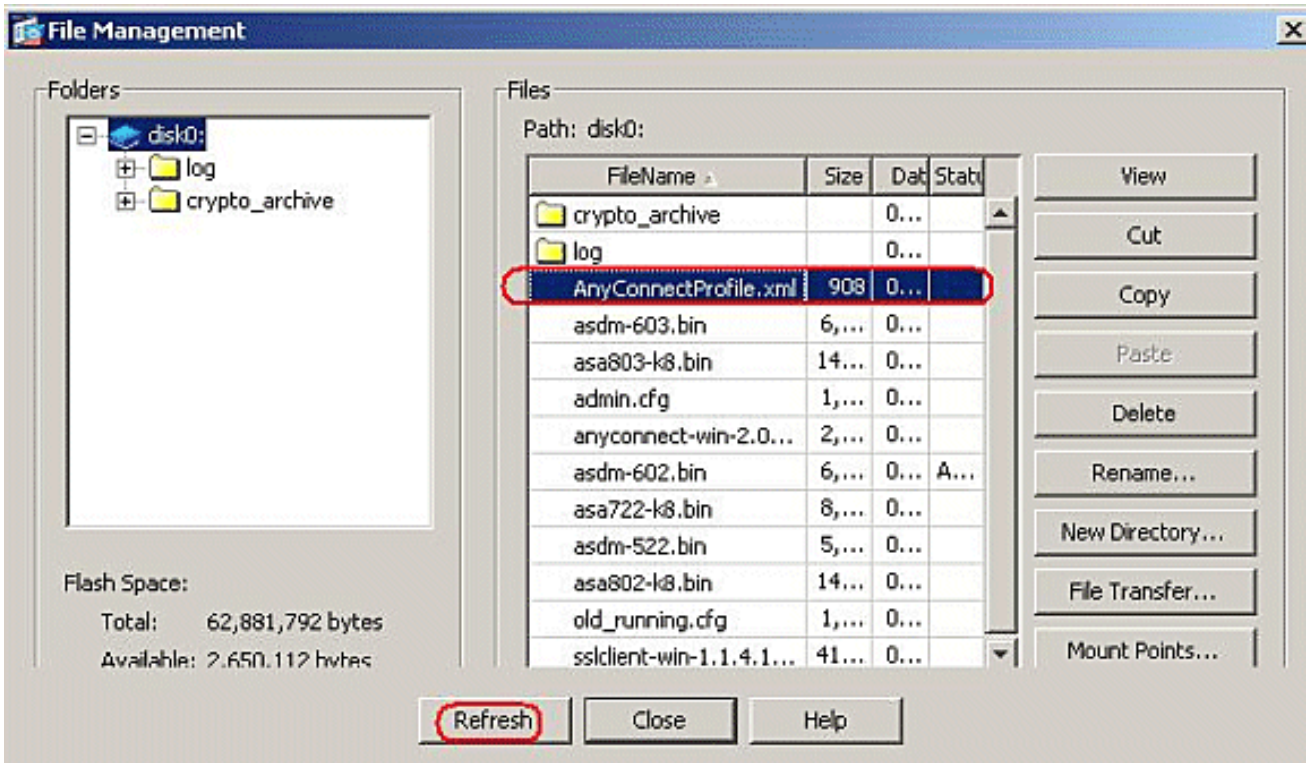
8. 按一下**File Transfer**按鈕。



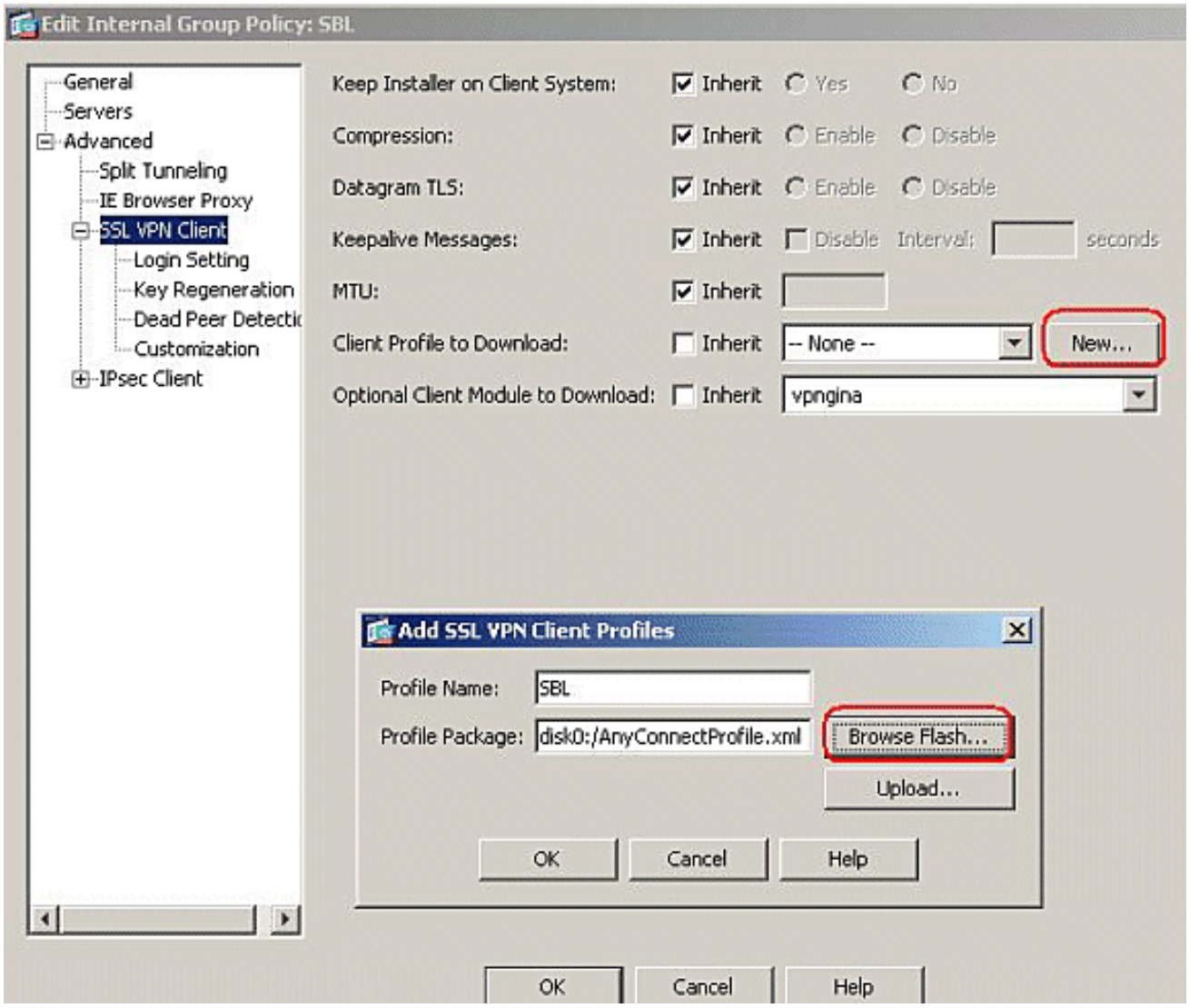
9. 要將配置檔案從本地電腦傳輸到ASA快閃記憶體，請根據需要選擇**Source File**、XML檔案（本地電腦）的路徑和**Destination File**路徑。



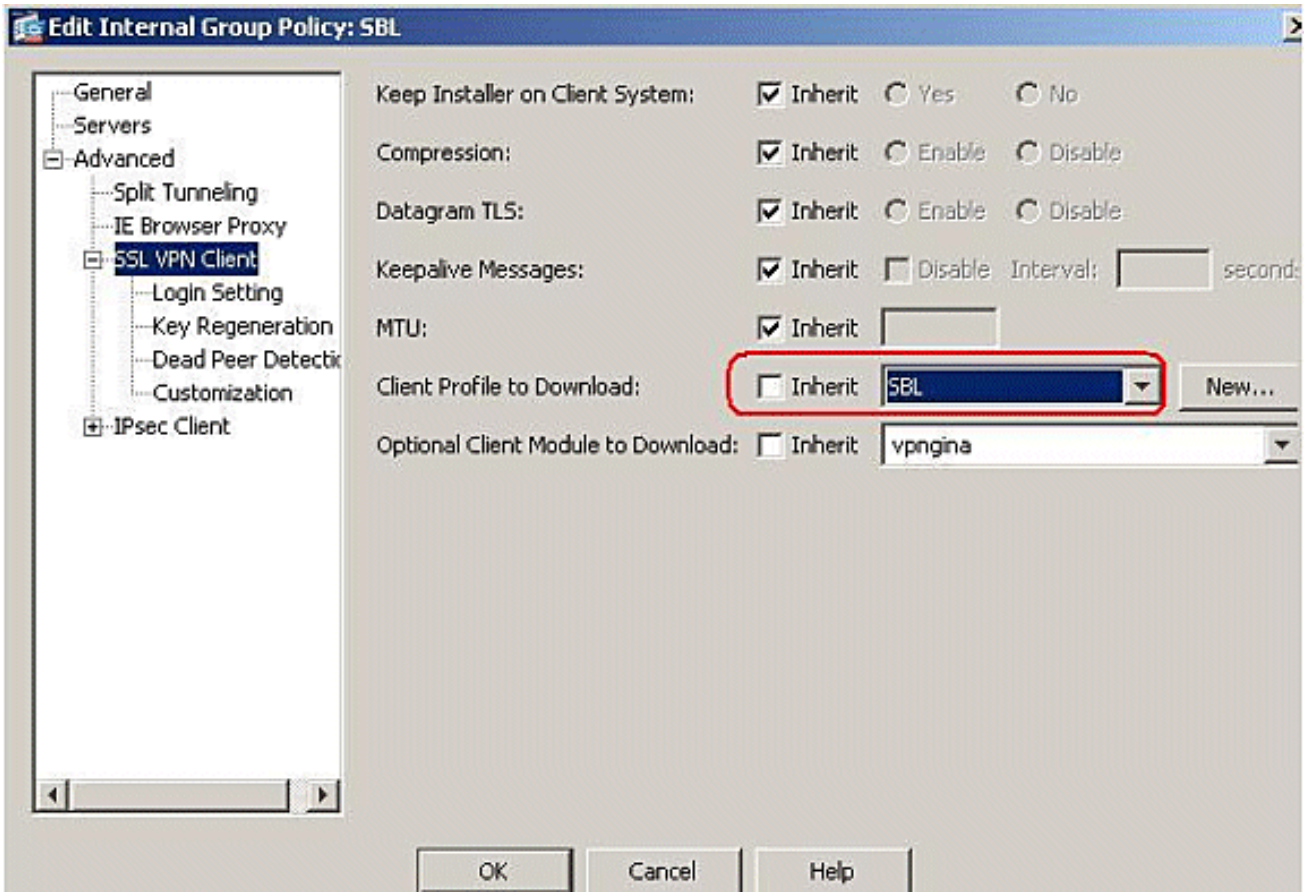
10. 傳輸後，按一下**Refresh**按鈕驗證配置檔案是否位於快閃記憶體中。



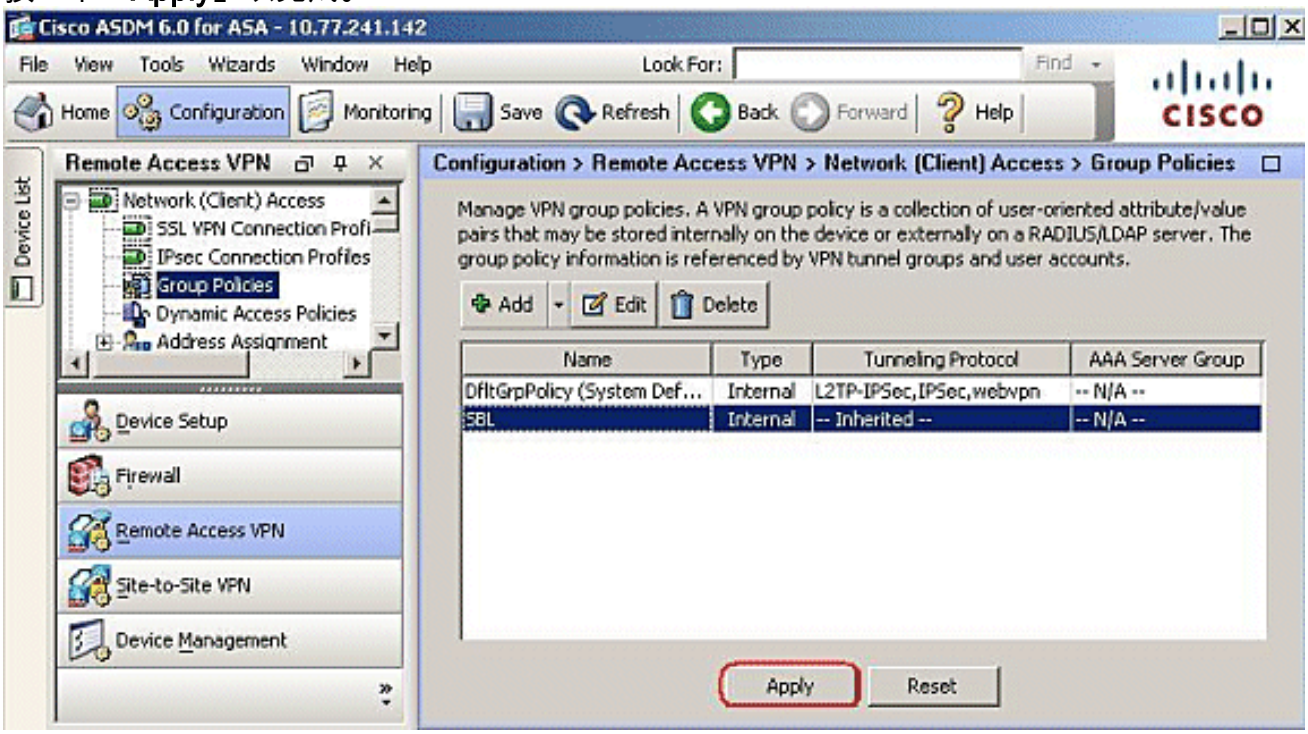
11. 將配置檔案分配到內部組策略(SBL)。按照以下路徑操作：**Configuration > Remote Access VPN > Network(Client)Access > Group Policies > Edit SBL(Internal Group Policy)> Advanced > SSL VPN Client > Client Profile to Download**，然後點選**New**按鈕。在**Add SSL VPN Client Profiles**中，按一下**Browse**按鈕以選擇儲存在ASA快閃記憶體中的配置檔案(**AnyConnectProfile.xml**)的位置。為配置檔案指定**Name**，例如**SBL**。按一下「**OK**」以完成。



12. 刪除Inherit覈取方塊並在**Client Profile to Download**欄位中選擇**SBL**。按一下「**OK**」（確定）。



13. 按一下「Apply」以完成。



使用清單檔案

在安全裝置上上載的AnyConnect軟體包包含名為VPNManifest.xml的檔案。此示例顯示此檔案的示例內容：

```
<?xml version="1.0" encoding="UTF-7"?> <vpn rev="1.0">
<file version="2.1.0150" id="VPNCore"
   is_core="yes" type="exe" action="install">
```

```
   <uri>binaries/anyconnect-win-2.1.0150-web-deploy-k9.exe</uri>
 </file>
 <file version="2.1.0150" id="gina"
   is_core="yes" type="exe" action="install" module="vpngina">
   <uri>binaries/anyconnect-gina-win-2.1.0150-web-deploy-k9.exe</uri>
 </file>
</vpn>
```

正如步驟1所述，安全裝置已在其上儲存已配置的配置檔案，並且還儲存一個或多個AnyConnect軟體包，其中包含AnyConnect客戶端自身、下載程式實用程式、清單檔案以及任何其他可選模組或支援檔案。

當遠端使用者通過WebLaunch或當前獨立客戶端連線到安全裝置時，下載程式首先下載並運行。它使用清單檔案來確定遠端使用者PC上是否存在需要升級的當前客戶端，或者是否需要全新安裝。清單檔案還包含關於是否有任何必須下載和安裝的可選模組（在本例中為VPNGINA）的資訊。客戶端配置檔案也會從安全裝置向下推送。VPNGINA的安裝由在**group-policy(webvpn)**命令模式下配置的**svc modules value vpngina**命令啟用，如步驟4所述。AnyConnect客戶端和VPNGINA已安裝，並且使用者在Windows域登入之前在下次重新啟動時看到AnyConnect客戶端。

當使用者連線時，客戶端和配置檔案被向下傳遞到使用者PC;安裝客戶端和VPNGINA;使用者可在下次重新啟動時（登入之前）看到AnyConnect客戶端。

安裝AnyConnect時，客戶端PC上提供了一個示例配置檔案：**C:\Documents and Settings\All使用者\應用程式Data\Cisco\Cisco\AnyConnect VPN Client\Profile\AnyConnectProfile**。

排除SBL故障

如果您遇到SBL問題，請使用以下步驟：

1. 確保已推送配置檔案。
2. 刪除以前的配置檔案；在硬碟上搜尋它們以查詢位置：*.xml。
3. 轉到「新增/刪除程式」時，您是否同時安裝了AnyConnect和AnyConnect VPNGINA?
4. 解除安裝AnyConnect客戶端。
5. 在事件檢視器中清除使用者的AnyConnect日誌並重新測試。
6. Web瀏覽回到安全裝置以重新安裝客戶端。
7. 確保也顯示配置檔案。
8. 重新啟動一次。下次重新啟動時，系統將提示您輸入Start Before Logon提示。
9. 以.evt格式將AnyConnect事件日誌傳送到思科。
10. 如果您看到此錯誤，請刪除使用者配置檔案並使用預設配置檔案：

```
Description: Unable to parse the profile
C:\Documents and Settings\All Users\Application Data\Cisco
\Cisco AnyConnect VPN Client\Profile\VABaseProfile.xml.
Host data not available.
```

問題1

嘗試上傳AnyConnect配置檔案時出現以下錯誤消息：XML。如何解決此錯誤？

解決方案1

出現此錯誤消息的主要原因是AnyConnect配置檔案中的語法或配置問題。為了解決此問題，請確保

配置的AnyConnect配置檔案與Cisco AnyConnect VPN客戶端管理員指南的Sample AnyConnect Profile and XML Schema部分中提供的示例AnyConnect配置檔案相似。

相關資訊

- Cisco AnyConnect VPN客戶端管理員指南2.0版
- 建立登入指令碼 — Windows TechNet
- 在Windows Vista系統上配置登入前啟動(PLAP)
- 使用AnyConnect SSL VPN客戶端的ASA 8.x VPN訪問配置示例
- Cisco AnyConnect VPN使用者端
- Cisco ASA 5500系列調適型安全裝置
- 技術支援與文件 - Cisco Systems